UNITED STATES PATENT AND TRADEMARK OFFICE

A

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/626,637	07/27/2000	Deepak Gupta	JP920000150US1	9799

39903 7590 08/11/2005

ANTHONY ENGLAND
PO Box 5307
AUSTIN, TX 78763-5307

EXAMINER	
SHIN, KYUNG H	

ART UNIT	PAPER NUMBER
2143	

DATE MAILED: 08/11/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/626,637	GUPTA ET AL.	
	Examiner	Art Unit	
	Kyung H. Shin	2143	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *11 April 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-6 and 11-19* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-6 and 11-19* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *27 July 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *9/23,10/22/04*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. In view of the Appeal Brief filed on 4/11/2005, PROSECUTION IS HEREBY REOPENED. A new ground of rejection is set forth below.

To avoid abandonment of the application, appellant must exercise one of the following two options:

(1) file a reply under 37 CFR 1.111 (if this Office action is non-final) or a reply under 37 CFR 1.113 (if this Office action is final); or,

(2) request reinstatement of the appeal.

If reinstatement of the appeal is requested, such request must be accompanied by a supplemental appeal brief, but no new amendments, affidavits (37 CFR 1.130, 1.131 or 1.132) or other evidence are permitted. See 37 CFR 1.193(b)(2).

2. Claims **1 - 6, 11 - 19** are pending. Claims **1 - 5** are amended. Claims **7 - 10** are cancelled. Claims **11 - 19** are new. Independent claims are **1, 6, 13**.

Claim Rejection - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and

the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. **Claims 1, 4 - 6, 11, 13, 17 - 19** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Lewis et al.** (US Patent No. 6,233,565) in view of **Weinstein et al.** (US Patent No. 6,094,485).

Regarding Claim 1 (Currently Amended), Lewis discloses a method for enabling the use by a browser of valid authentication certificates in relation to a transaction between the browser and a server when a private key and public key of a certifying authority of the server has expired, comprising:

b) verifying by the browser the original authentication certificate using the expired public key of the certifying authority, (see Lewis col. 14, lines 36-42; col. 30, lines 41-43: verify certificate by (i.e. client) browser using expired public key for verification and utilize expired private key for digital signature generation) and

c) verifying by the browser the SCAC certificate using a new public key of the certifying authority. (see Lewis col. 30, lines 43-50: verify certificate by (i.e. client) browser using new public key for verification and new private key for digital signature generation)

Lewis discloses wherein receiving an original authentication certificate and a server certifying authority chain (SCAC) certificate by the browser from the server during a SSL handshake between the browser and the server, said SCAC certificate having been previously obtained by the server from the certifying

authority (see Lewis col. 30, lines 39-41; col. 14, lines 36-42; col. 15, lines 42-46: receive original certificate, new certificate utilizing SSL techniques)

Lewis does not specifically disclose certificates received together. However, Weinstein discloses:

a) receiving an original authentication certificate together with a server certifying authority chain (SCAC) certificate. (see Weinstein col. 3, lines 56-64: multiple (i.e. new, intermediate (i.e. old)) certificates within a transmission (i.e. together))

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Lewis to enable multiple security client/server certificates transmitted within a network session as taught by Weinstein. One of ordinary skill in the art would be motivated to employ Weinstein in order to optimize encryption within a secure network communications session. (see Weinstein col. 2, lines 10-15: " *... provides a process and apparatus that is used by an exportable version of an SSL client ... negotiate an encrypted communication session using strong encryption with an SSL server ...* ")

Regarding Claim 5 (Currently Amended), Lewis discloses the method of claim 1, wherein the method further comprises presenting the CCAC certificate to the server during the handshake. (see Lewis col. 14, lines 36-42; col. 15, lines 42-46; col. 31, lines 5-21: certificate to contain client public/private key pair generated and client certificate setup utilizing handshake (i.e. SSL) techniques)

Regarding Claim 6 (Original), Lewis discloses in an arrangement of networked server and browser systems conducting secure transactions and including a certifying authority for authenticating such transactions, characterized in that it includes a means for authenticating transactions when the public and private key of the said certifying authority have expired but the authentication certificates of any of server or browser systems is still valid, comprising;

a) a means for the server to obtain a certifying authority chain certificate using the new private key of the certifying authority, (see Lewis col. 30, lines 39-41: server receives a new certificate designating a new private key)

c) a means for verifying the original authentication certificate using the expired public key of the certifying authority, and verifying the certifying authority chain certificate using the new certifying authority public key by the browser. (see Lewis col. 30, lines 43-50: initial certificate signed with expired private key (i.e. verified with expired public key), new certificate signed with new private key (i.e. verified with new public key))

Lewis discloses the usage of original and new certificates. (see Lewis col. 14, lines 36-42; col. 30, lines 41-43: certificates utilized for authenication) Lewis does not specifically disclose certificates received together. However, Weinstein discloses:

b) a means for presenting the said certifying authority chain certificate together with the original authentication certificate, to the browser; (see Weinstein col. 3, lines 56-64: multiple (i.e. new, intermediate (i.e. old)) certificates within a transmission)

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Lewis to enable multiple security client/server certificates transmitted within a network session as taught by Weinstein. One of ordinary skill in the art would be motivated to employ Weinstein in order to optimize encryption within a secure network communications session. (see Weinstein col. 2, lines 10-15)

Regarding Claims 11 (New), **18** (New), Lewis discloses the method and system of claims 1, 13 further comprising accepting the transaction by the browser after said verifying the original authentication certificate and after said verifying the SCAC certificate. (see Lewis col. 27, lines 10-24: verification of a certificate (i.e. server or client) utilizing digital signature techniques with public/private keys)

Regarding Claims 12 (New), **19** (New), Lewis disclose the method and system of claims 1, 13, wherein obtaining the SCAC certificate comprises using the new private key of the certifying authority. (see Lewis col. 30, lines 41-43: certificate (i.e. server/client) utilizing private key for digital signature generation and public key for verification)

Regarding Claim 13 (New), Lewis discloses a system for enabling use by a browser of valid authentication certificates in relation to a transaction between the browser and a

server when a private key and public key of a certifying authority of the server has expired, comprising:

b) means for verifying by the browser the original authentication certificate using the expired public key of the certifying authority; (see Lewis col. 30, lines 43-50: initial certificate signed with expired private key (i.e. verified with expired public key), new certificate signed with new private key (i.e. verified with new public key)) and

c) means for verifying by the browser the SCAC certificate using a new public key of the certifying authority. (see Lewis col. 30, lines 39-41: server receives a new certificate designating a new private key)

Lewis discloses wherein means for receiving an original authentication certificate and a server certifying authority chain (SCAC) certificate by the browser from the server during a SSL handshake between the browser and the server, said SCAC certificate having been previously obtained by the server from the certifying authority; (see Lewis col. 30, lines 39-41; col. 14, lines 36-42; col. 15, lines 42-46: receive original certificate, new certificate utilizing SSL techniques) Lewis does not specifically disclose certificates received together. However, Weinstein discloses:

a) receiving an original authentication certificate together with a server certifying authority chain (SCAC) certificate. (see Weinstein col. 3, lines 56-64: multiple (i.e. new, intermediate (i.e. old)) certificates within transmission)

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Lewis to enable multiple security client/server certificates transmitted within a network session as taught by Weinstein. One of ordinary skill in the art would be motivated to employ Weinstein in order to optimize encryption within a secure network communications session. (see Weinstein col. 2, lines 10-15)

Regarding Claim 17 (New), Lewis discloses the system of claim 13, wherein the system further comprises means for presenting the CCAC certificate to the server during the handshake. (see Lewis col. 14, lines 36-42; col. 15, lines 42-46; col. 31, lines 5-21: certificate to contain client public/private key pair generated and client certificate setup utilizing handshake (i.e. SSL) techniques)

5. **Claims 2, 3, 14, 15** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Lewis-Weinstein** and further in view of **Perlman et al.** (US Patent No. 6,230,266).

Regarding Claim 2 (Currently Amended), Lewis discloses a Certificate Authority (CA) for the distribution of certificates used in the verification of client and server systems. Lewis does not disclose a Certificate Authority (CA) that invalidates or withdraws its public/private key. However, Perlman discloses Certificate Authority (CA) that invalidates or withdraws its public/private key pair through the process of revocation.

Further, Perlman discloses the method of claim 1, wherein the SCAC certificate is obtained by the server whenever the certifying authority invalidates its public key, wherein the certificate is obtained by:

a) contacting the certifying authority using the server's private key for authentication to make a request for the SCAC certificate; (see Perlman col. 6, line 63 - col. 7, line 6: contact CA concerning certificate revocation)

b) verifying the request by the certifying authority using the server's public key; (see Perlman col. 7, lines 15-18: verify key revocation) and

c) generating the SCAC certificate by the certifying authority using it's new private key of the certifying authority and forwarding the SCAC certificate to the server. (see Perlman col. 7, lines 12-24: update certificate information, attach key to new certificate)

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the inventions of Lewis to include a Certificate Authority (CA) that invalidates its key pair through the process of revocation as taught by Perlman. One of ordinary skill in the art would have been motivated to employ Perlman in order to ensure the authenticity of certificates when a CA invalidates a public/private key pair. (see Perlman col. 2, lines 20-26: *" ... network security, every principal must have a certificate ... desirable to later disable a certificate after it has been issued but prior to its expiration. For example, a principal's private key may be stolen, compromised or lost, etc. ... revoke the certificate, thereby disabling authentication via that certificate ... "*)

Regarding Claim 3 (Currently Amended), Lewis discloses a Certificate Authority (CA) for the distribution of certificates used in the verification of client and server systems and an entity (i.e. server) name for a certificate. (see Lewis col. 26, line 56: entity (i.e. server) name within certificate) Lewis does not disclose usage of the server public key, CA name and public key in the authentication process. However, Perlman discloses the method of claim 2 wherein generating the SCAC certificate includes authenticating the server public key, old certifying authority public key and certifying authority name. (see Perlman col. 7, lines 10-12: public keys, CA name)

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the inventions of Lewis to include the invention of Perlman enable usage. One of ordinary skill in the art would have been motivated to employ the invention of Perlman to Lewis in order to use efficiently the server name and public key, CA name and public key authentication. (see Perlman col. 1, line 65 - col. 2, line 9: " *... reliably know which public key belongs to which principal ... CA generates identity certificates ... specifying ... name of the principal whose public key is being certified, the certificate serial number, name of the CA issuing the certificate, the subject's public key, and also, typically, a certificate expiration date ... relationship between the public key and the principal to which it belongs precludes an intruder from compromising the system by posing as a valid principal ...* " ; col. 7, lines 10-12: " *... new CA 204b is configured to issue certificates in the same name as the CA 204a ...* ") The compromise of a CA and its identifying information requires another CA and its

identifying information to assume the certificate verification process.

Regarding Claim 14 (New), Lewis does not disclose a Certificate Authority (CA) invalidation of it public/private key. However, Perlman discloses the system of claim 13, wherein the SCAC certificate is obtained by the server whenever the certifying authority invalidates its public key, wherein the certificate is obtained by:

a) means for contacting the certifying authority using the server's private key for authentication to make a request for the SCAC certificate; (see Perlman col. 6, line 63 - col. 7, line 6: contact CA concerning certificate revocation)

b) means for verifying the request by the certifying authority using the server's public key; (see Perlman col. 7, lines 15-18: verify key revocation) and

c) means for generating the SCAC certificate by the certifying authority using a new private key of the certifying authority and forwarding the SCAC certificate to the server. (see Perlman col. 7, lines 12-24: update certificate information, attach key to new certificate)

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the inventions of Lewis to include a Certificate Authority (CA) that invalidates its key pair as taught by Perlman. One of ordinary skill in the art would have been motivated to employ Perlman in order to ensure the authenticity of certificates when a CA invalidates a public/private key pair to a compromise in security. (see Perlman col. 2, lines 20-26)

Regarding Claim 15 (New), Lewis discloses a Certificate Authority (CA) for the distribution of certificates used in the verification of client and server systems. Lewis discloses an entity (i.e. server) name for a certificate. (see Lewis col. 26, line 56: entity (i.e. server) name within certificate) Lewis does not specifically disclose usage of the public key, CA name and public key in the authentication process. However, Perlman discloses the system of claim 13, wherein said means for generating the SCAC certificate includes means for authenticating the server name, the server public key, old certifying authority public key, and certifying authority name. (see Perlman col. 7, lines 10-12: public keys, CA name)

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the inventions of Lewis to employ the certificates includes the authentication of the server public key, old CA public key and CA name as taught by Perlman. One of ordinary skill in the art would have been motivated to employ Perlman in order to efficiently and securely re-establish authentication system by using the server name and public key, CA name and public key authentication. (see Perlman col. 3, lines 54-63)

6. **Claim 4** is rejected under 35 U.S.C. 103(a) as being unpatentable over **Lewis-Weinstein** and further in view of **Kramer et al.** (US Patent No. 6,324,525).

Regarding Claim 4 (Currently Amended), Lewis discloses the usage of certificates for entity authentication. (see Lewis col. 31, lines 35-38: client/server certificate usage for

authentication) Lewis does not specifically disclose the usage of a Certificate Authority (CA) issuing client and server type certificates. However, Kramer discloses the method of claim 1 further comprising issuing by the certifying authority a client (CCAC) certificate, said CCAC certificate being functionally the same as the SCAC certificate subject to the roles of the browser and the server being interchanged. (see Kramer col. 105, lines 61-62; col. 105, line 66 - col. 106, line 1; col. 90, lines 27-31: Certificate Authority (CA) for certificate issuance; col. 17, lines 43-47; col. 17, lines 27-30: client and server type certificates)

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Lewis to enable the usage of client and server certificates utilizing a trusted third party designated a certificate authority for certificate issuance as taught by Kramer. One of ordinary skill in the art would be motivated to employ Kramer in order to enable secure communications over the publicly access network such as the Internet communications network. (see Kramer col. 4, lines 19-21: " ... *critical that any solution utilizing the Internet for a communication backbone employ some form of cryptography* ... ")

7. **Claim 16** is rejected under 35 U.S.C. 103(a) as being unpatentable over **Lewis-Weinstein-Perlman** and further in view of **Kramer et al.** (US Patent No. 6,324,525).

Regarding Claim 16 (New), Lewis discloses the usage of certificates for entity authentication. (see Lewis col. col. 30, lines 59-62:) Lewis does not specifically

disclose the usage of a Certificate Authority issuing client and server type certificate. However, Kramer discloses the system of claim 15, further comprising means for issuing by the certifying authority a client (CCAC) certificate, said CCAC certificate being functionally the same as the SCAC certificate subject to the roles of the browser and the server being interchanged. (see Kramer col. 105, lines 61-62; col. 105, line 66 - col. 106, line 1; col. 90, lines 27-31: Certificate Authority (CA) for certificate issuance; col. 17, lines 43-47; col. 17, lines 27-30: client and server certificates)

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Lewis to enable the usage of client certificates and server certificates utilizing a trusted third party designated a certificate authority for certificate issuance as taught by Kramer. One of ordinary skill in the art would be motivated to employ Kramer in order to enable secure communications over the publicly access network such as the Internet communications network. (see Kramer col. 4, lines 19-21)

Conclusion

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kyung H. Shin whose telephone number is (571) 272-3920. The examiner can normally be reached on 9 am - 7 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, David A. Wiley can be reached on (571) 272-3923. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

KHS
Kyung H Shin
Patent Examiner
Art Unit 2143

KHS
August 7, 2005

DAVID WILEY
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100